Unbounded randomness certification using sequences of measurements

PHYSICAL REVIEW A **95**, 020102(R) (2017)

Unbounded randomness certification using sequences of measurements

F. J. Curchod,[1,*] M. Johansson,[1,†] R. Augusiak,[2] M. J. Hoban,[3] P. Wittek,[1,4] and A. Acín[1,5]

[1]*ICFO-Institut de Ciencies Fotoniques, Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain*

[2]*Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotników 32/46, 02-668 Warsaw, Poland*

[3]*Department of Computer Science, University of Oxford, Oxford OX1 3QD, United Kingdom*

[4]*University of Borås, 50190 Borås, Sweden*

[5]*ICREA–Institució Catalana de Recerca i Estudis Avançats, E-08010 Barcelona, Spain*

(Received 20 November 2015; revised manuscript received 25 November 2016; published 17 February 2017)

Unpredictability, or randomness, of the outcomes of measurements made on an entangled state can be *certified* provided that the statistics violate a Bell inequality. In the standard Bell scenario where each party performs a single measurement on its share of the system, only a finite amount of randomness, of at most $4\log_2 d$ bits, can be certified from a pair of entangled particles of dimension d. Our work shows that this fundamental limitation can be overcome using sequences of (nonprojective) measurements on the same system. More precisely, we prove that one can certify *any* amount of random bits from a pair of qubits in a pure state as the resource, even if it is arbitrarily weakly entangled. In addition, this certification is achieved by near-maximal violation of a particular Bell inequality for each measurement in the sequence.

DOI: 10.1103/PhysRevA.95.020102

Introduction. Bell's theorem [1] has shown that the predictions of quantum mechanics demonstrate nonlocality. That is, they cannot be described by a theory in which there are objective properties of a system prior to measurement that satisfy the no-signaling principle (sometimes referred to as "local realism"). Thus, if one requires the no-signaling principle to be satisfied at the operational level then the outcomes of measurements demonstrating nonlocality must be unpredictable [1–3]. This unpredictability, or randomness, is not the result of ignorance about the system preparation but is *intrinsic* to the theory.

Although the connection between quantum nonlocality (via Bell's theorem) and the existence of intrinsic randomness is well known [1–4] it was analyzed in a quantitative way only recently [5,6]. It was shown how to use nonlocality (probability distributions that violate a Bell inequality) to *certify* the unpredictability of the outcomes of certain physical processes. This was termed *device-independent randomness certification*, because the certification only relies on the statistical properties of the outcomes and not on how they were produced. The development of information protocols exploiting this certified form of randomness, such as device-independent randomness expansion [5–7] and amplification protocols [8,9], followed.

Entanglement is a necessary resource for quantum nonlocality, which in turn is required for randomness certification. It is thus crucial to understand qualitatively and quantitatively how these three fundamental quantities relate to one another. In our work, we focus on asking how much certifiable randomness can be obtained from a single entangled state as a resource. Progress has been made in this direction for entangled states shared between two parties, Alice (A) and Bob (B), in the standard scenario where each party makes a single measurement on his share of the system and then discards it. An argument adapted from Ref. [10] shows that either of the two parties, (A) or (B), can certify at most $2\log_2 d$ bits of randomness [11], where d is the dimension of the local Hilbert space the state lives in, which in turn implies a bound of $4\log_2 d$ bits when the two outputs are combined. This demonstrates a fundamental limitation for device-independent randomness certification in the standard scenario. The main goal of our work is to show that this limitation on the amount of certifiable random bits from one quantum state can be lifted. To do this we will consider the sequential scenario, where sequences of measurements can be applied to each local system. Our main result is to prove that an unbounded amount of random bits can be certified in this scenario.

To gain intuition, consider the following setup where, contrary to the device-independent approach followed here, the functioning of a device can be entirely trusted. The device consists of a quantum state prepared in the Pauli-Z or σ_z eigenstate $|0\rangle$ followed by a measurement in the Pauli-X or σ_x basis $\{|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}\}$. The outcome of this measurement is random and if the device then makes another measurement on the output state, this time in the Pauli-Z basis, it gives yet another random outcome. In this fashion of alternating between the two orthogonal bases, one can potentially obtain an unbounded number of random bits from one qubit. The limitation of this procedure for producing random numbers is that one cannot distinguish this device from a classical one with preprogrammed outcomes—a *local model* for the outcomes—if one does not fully trust the functioning of the device.

Clearly we cannot *certify* any randomness from a single system (in a device-independent manner) as in the above example, since one needs nonlocality for this purpose. But is it possible to build a scheme that exploits nonlocality and makes use of this idea of measuring the state repeatedly to overcome the bound on the amount of certifiable randomness that one can obtain from a single entangled quantum system? To do so, the main obstacle comes from the fact that the local measurements needed to generate the random outcomes destroy the entanglement present in the state (and nonlocality in the correlations). Thus, one of the challenges is to come up with nondestructive measurements that still produce nonlocality but

*florian.curchod@icfo.es

†markus.johansson@icfo.es

retain some entanglement in the postmeasurement state. In this way, the state can still be used as a resource for subsequent measurements.

Bell tests with sequences of measurements have received less attention than the standard ones with a single measurement round in the literature despite the novel features in this scenario [12], as for example the phenomenon known as hidden nonlocality [13]. In our work we show that they prove useful in the task of randomness certification, which also provides another example [11] where general measurements can overcome limitations of projective ones. More precisely, we describe a scheme where any number m of random bits are certified using a sequence of $n > m$ consecutive measurements on the same system. This work thus shows that the bound of $4\log_2 d$ random bits in the standard scenario can be overcome in the sequential scenario, where it is impossible to establish any bound. The unbounded randomness is certified by a near-maximal violation of a particular Bell inequality for each measurement in the sequence. Moreover, for any finite amount of certified randomness, our protocol has a finite (yet very small) noise robustness.

Sequential measurements scenario. Before presenting our results, let us introduce the scenario we work in. We carry over many of the features from the standard scenario except now we allow party B to make multiple measurements in a sequence on his share of the state. One can visualize this as in Fig. 1 where B is split up into several Bs, each one corresponding to a measurement made on the state and labeled by $B_i, i \in \{1,2,\ldots,n\}$, where n is the total number of measurements made in the sequence. Each B_i makes one measurement and the postmeasurement state is sent to B_{i+1}. We organize the Bobs such that B_i is doing his measurement *before* B_j for $i < j$. Thus in principle B_j can receive the information about the inputs and outputs of previous measurements B_i for all $i < j$.

To quantify the randomness produced in the setup, we put the above scenario in the setting of *nonlocal guessing games* (e.g., Refs. [11,14–16]). Let us consider an additional

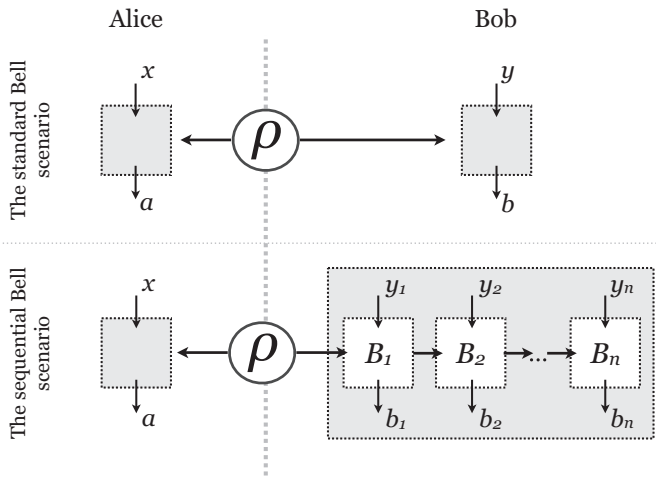

FIG. 1. The standard scenario where parties A and B make a single quantum measurement on their share of the state and discard it versus the sequential scenario where the second party B makes multiple measurements on his share.

adversary Eve (E) who is in possession of a quantum system potentially correlated to the one of A and B. The global state is denoted ρ_{ABE}. We assume that at each round of the experiment, E is the one preparing the state ρ_{ABE} and distributes $\rho_{AB} = \mathrm{Tr}_E \rho_{ABE}$ to A and B. This state will be used to make the measurements in the sequence and the aim of E is to try to guess B's outcomes by using measurements on her share of the state ρ_{ABE}. The parties A and B_i, having no knowledge about the state or the real measurements made on it, see their respective devices as black boxes that receive some classical input $x \in \{0,1\}$ and $y_i \in \{0,1\}$, $y_1, y_2, \ldots, y_n \equiv \vec{y}$, respectively, and that generate a classical output $a \in \{\pm 1\}$ and $b_i \in \{\pm 1\}$, $(b_1, b_2, \ldots, b_n) \equiv \vec{b}$, respectively (see Fig. 1). They generate statistics from multiple runs of the experiment to obtain the observed probability distribution P_{obs} with elements $p_{\mathrm{obs}}(a,\vec{b}|x,\vec{y})$. This distribution P_{obs} lives inside the set of quantum correlations $\mathcal{Q}$ obtained from measurements on quantum states in a sequence as we described. This set is convex and thus can be described in terms of its extreme points, denoted P_{ext}, and any P_{obs} can be written as $P_{\mathrm{obs}} = \sum_{\mathrm{ext}} q_{\mathrm{ext}} P_{\mathrm{ext}}$, where $\sum_{\mathrm{ext}} q_{\mathrm{ext}} = 1$ and every $q_{\mathrm{ext}} \geqslant 0$.

From studying the outcome statistics *only* we can bound E's predictive power by allowing her to have complete knowledge of how P_{obs} is decomposed into extreme points, i.e., she knows the probability distribution q_{ext} over extreme points P_{ext}. This predictive power is quantified via the *device-independent guessing probability* (DIGP) [14] where we fix the particular input string $y_1^0, y_2^0, \ldots, y_n^0 \equiv \vec{y}^0$ for which E has to guess the outputs $\vec{b}$. The DIGP, denoted by $G(\vec{y}^0, P_{\mathrm{obs}})$, is then calculated as the optimal solution to the following optimization problem [15,16]:

$$G(\vec{y}^0, P_{\mathrm{obs}}) = \max_{\{q_{\mathrm{ext}}, P_{\mathrm{ext}}\}} \sum_{\mathrm{ext}} q_{\mathrm{ext}} \max_{\vec{b}} p_{\mathrm{ext}}(\vec{b}|\vec{y}^0),$$

subject to

$$p_{\mathrm{ext}}(\vec{b}|\vec{y}^0) = \sum_a p_{\mathrm{ext}}(a,\vec{b}|x,\vec{y}^0), \quad \forall\, x, \tag{1}$$

$$P_{\mathrm{obs}} = \sum_{\mathrm{ext}} q_{\mathrm{ext}} P_{\mathrm{ext}}, \quad P_{\mathrm{ext}} \in \mathcal{Q}. \tag{2}$$

The operational meaning of this quantity is clear: Eve has a complete description of the observed correlations in terms of extreme points. She then guesses the most probable outcome for each extreme point. The standard scenario with a single measurement round can also be represented in this formalism by simply considering that $\vec{b} = b$ and $\vec{y}^{(0)} = y^{(0)}$. To quantify the amount of bits of randomness that is certified, we use the *min entropy* $H(\vec{y}^0, P_{\mathrm{obs}}) = -\log_2 G(\vec{y}^0, P_{\mathrm{obs}})$ which returns m bits of randomness if $G(\vec{y}^0, P_{\mathrm{obs}}) = 2^{-m}$. The amount of bits of randomness quantified in this way is the figure of merit in this work and our goal is to obtain as many bits as possible from a single system.

In what follows, problem (2) is relaxed to an optimization where instead of insisting on $P_{\mathrm{obs}} = \sum_{\mathrm{ext}} q_{\mathrm{ext}} P_{\mathrm{ext}}$ (2), we only impose that the observed statistics P_{obs} give a particular Bell inequality violation [5]. The optimal solution to this new problem is an upper bound to the optimal solution of Eq. (2).

Crucially, this relaxation still gives good bounds as shown below.

Before presenting our results, it is worth explaining why the causal constraints imposed by the sequential scenario make it stronger than standard Bell tests. At first sight, one could be tempted to group all the measurements in the sequence into a single box receiving an input string $\vec{y}_n$ to output another string $\vec{b}_n$, as in a standard Bell test. However, in general a sequence of measurements cannot be represented as a single measurement. To understand this, note that in the sequential scenario the outcome b_i can depend only on variables produced in its past, namely, the input choices $y_1, y_2, \ldots, y_i$ and the outcomes $b_1, b_2, \ldots, b_{i-1}$ that were *previously* obtained. However, in the single measurement scenario, the measurement box receives all inputs and produces all outputs at once. In particular, outcome b_i can now be a function of input choices $y_{j>i}$ and outcomes $b_{j>i}$ that are produced in the *future*. That is, such a big box may violate the physical constraints coming from the sequential arrangement and the assumption that signaling from the future to the past is impossible. These additional causality constraints further limit Eve's predictability with respect to a standard Bell test and are responsible of the unbounded amount of certified randomness.

Ingredients. Alice and Bob share the pure two-qubit state

$$|\psi(\theta)\rangle = \cos(\theta)|00\rangle + \sin(\theta)|11\rangle \tag{3}$$

that for all $\theta \in]0,\pi/2[$ is entangled. In Ref. [14], a family of Bell inequalities was introduced:

$$I_\theta = \beta\langle\mathbb{B}_0\rangle + \langle\mathbb{A}_0\mathbb{B}_0\rangle + \langle\mathbb{A}_1\mathbb{B}_0\rangle + \langle\mathbb{A}_0\mathbb{B}_1\rangle - \langle\mathbb{A}_1\mathbb{B}_1\rangle, \tag{4}$$

where $\beta = 2\cos(2\theta)/[1+\sin^2(2\theta)]^{1/2}$, $\langle\mathbb{B}_y\rangle = p(b=+1|y) - p(b=-1|y)$ and $\langle\mathbb{A}_x\mathbb{B}_y\rangle = p(a=b|xy) - p(a\neq b|xy)$ for $x, y \in \{0,1\}$. This family of inequalities has the following two useful properties: First, its maximal quantum violation, $I_\theta^{\max} = 2\sqrt{2}\sqrt{1+\beta^2/4}$, is obtained by measuring the state (3) with the measurements

$$\begin{aligned} \mathbb{A}_0 &= \cos\mu\,\sigma_z + \sin\mu\,\sigma_x, \quad \mathbb{B}_0 = \sigma_z, \\ \mathbb{A}_1 &= \cos\mu\,\sigma_z - \sin\mu\,\sigma_x, \quad \mathbb{B}_1 = \sigma_x, \end{aligned} \tag{5}$$

where $\tan\mu = \sin(2\theta)$. Second, when maximally violated, the inequality certifies one bit of local randomness on Bob's side for his second measurement choice $y^0 = 1$: $G(y^0 = 1, P_{\text{obs}}^{\max}) = 1/2$ [14]. These observations are possible because the maximal violation is *uniquely* achieved by the probability distribution $P_{\text{obs}}^{\max}$ that arises from the previously described state and measurements (3) and (5). Therefore, for the maximal violation, $P_{\text{obs}}^{\max} = P_{\text{ext}}$ in (2) and the guessing probability for input choice $y^0 = 1$ is equal to $1/2$.

However, in general we may not get correlations that maximally violate our Bell inequality but give a violation that is only close to maximal. In Secs. 1, 2, and 3 (found in the Supplemental Material [17]) we show how to make conclusions about the guessing probability for nonmaximal violations. In particular, we show that for *any* Bell inequality with a unique point of maximal violation, the guessing probability is a continuous function of the value of the inequality close to the maximal violation. This implies in the particular case we are studying that

$$I_\theta \to I_\theta^{\max} \Rightarrow G(y^0 = 1, P_{\text{obs}}) \to \tfrac{1}{2}. \tag{6}$$

In Sec. 6 in the Supplemental Material, we also provide a numerical upper bound on the guessing probability $G(y^0 = 1, P_{\text{obs}})$ by a concave function of the value of I_θ.

Bell inequalities (4) are the first main ingredient in our sequential construction below. The second one is the use of general, nonprojective measurements. Indeed, if B_1 performs a projective measurement on the shared entangled state, the resulting postmeasurement state, now shared between Alice and B_2, is separable and thus useless for randomness production. Consequently, one needs to consider nonprojective measurements to retain some entanglement in the system for the subsequent measurements. For this purpose, let us introduce the following two-outcome quantum measurement (written in the formalism of Kraus operators):

$$M_{\pm1}(\xi) = \cos\xi\,|\pm\rangle\langle\pm| + \sin\xi\,|\mp\rangle\langle\mp| \tag{7}$$

corresponding to the two outcomes $\{\pm1\}$. This measurement $\hat{\sigma}_x(\xi) \equiv \{M_{+1}^\dagger M_{+1}, M_{-1}^\dagger M_{-1}\}$ can be understood as a generalization of the projective measurement σ_x. It varies from being projective (for $\xi = 0$) to being noninteracting (for $\xi = \pi/4$). One can verify that measuring an entangled state (3) for $\xi \in]0,\pi/4]$ (nonprojective measurement) the post-measurement state still retains some entanglement, irrespective of the outcome. Therefore, by tuning the parameter ξ we are able to vary the destruction of the entanglement of the state at the gain of extracting information from it (cf. Ref. [18]): the closer to being a projective measurement, the lower the entanglement in the postmeasurement state, but the bigger the violation of the initial Bell inequality.

Scheme for unbounded randomness certification. We now combine the previous observations to demonstrate our main result. First, let us recall that, as shown in [14], one can obtain one bit of randomness from any pure entangled two qubit state, irrespective of the amount of entanglement in it. Moreover, one can verify that approximately one random bit can be certified if the measurements are close to the ones in Eq. (5) [in the sense that $\hat{\sigma}_x(\xi)$ is close to a measurement of σ_x for $\mathbb{B}_1$ in Eq. (5)] since I_θ is then close to $I_\theta^{\max}$ in Eq. (6). Second, the measurement in Eq. (7) is only close to projective for ξ close to zero and leaves entanglement in the postmeasurement state between Alice and Bob which is thus still useful for randomness certification. By repeated use of these two properties we can certify the production of an unbounded amount of random bits from a single pair of entangled qubits. We now formally describe this process in which Alice makes a single measurement on her share of the state, whereas Bob makes a sequence of n measurements on his.

Each B_i chooses between measurements of σ_z and $\hat{\sigma}_x(\xi_i)$ for inputs $y_i = 0$ and $y_i = 1$, respectively, with outcomes $b_i \in \{\pm1\}$. The parameter ξ_i is fixed before the beginning of the experiment. The initial entangled state shared between Alice and Bob, before B_1's measurement, is $|\psi^{(1)}(\theta_1)\rangle$ [see Eq. (3) with $\theta = \theta_1$]. If the first nonprojective measurement of the operator $\hat{\sigma}_x(\xi_1)$ is made by B_1 on the initial state $|\psi^{(1)}(\theta_1)\rangle$,

the postmeasurement state is of the form

$$\left|\psi^{(2)}_{b_1}(\theta_1,\xi_1)\right\rangle = U_A^{b_1}(\theta_1,\xi_1)\otimes V_B^{b_1}(\theta_1,\xi_1)(c|00\rangle + s|11\rangle), \quad (8)$$

where $c=\cos[\theta_{b_1}(\theta_1,\xi_1)]$ and $s=\sin[\theta_{b_1}(\theta_1,\xi_1)]$ and the two unitaries, $U_A^{b_1}(\theta_1,\xi_1)$ and $V_B^{b_1}(\theta_1,\xi_1)$, and angle $\theta_{b_1}(\theta_1,\xi_i)\in]0,\pi/4]$ depend on the first outcome b_1 and the angles θ_1 and ξ_1.

After his measurement, B_1 applies the unitary $(V_B^{b_1})^\dagger$, conditioned on his outcome b_1, on the postmeasurement state going to B_2. This allows B_2 to use the same two measurements $\hat{\sigma}(\xi_2)$ and σ_z independently of the outcome b_1 since the unitary $(V_B^{b_1})$ is canceled in Eq. (8). This last procedure will be applied by each B_i after his measurement, before sending the postmeasurement state to the next B_{i+1}. If the system passed through *only* the nonprojective measurements, the state received by B_i can be one of 2^{i-1} potential states, depending on all of the previous B_j's ($j<i$) outcomes [one for each combination $\vec{b}_{i-1}\equiv(b_1,b_2,\ldots,b_{i-1})$ of outcomes obtained by the previous B_j, these can be computed *before* the beginning of the experiment]. Any of these states can be written as

$$\left|\psi^{(i)}_{\vec{b}_{i-1}}\right\rangle = U_A^{\vec{b}_{i-1}}\otimes \mathbb{1}_B\left[\cos\left(\theta_{\vec{b}_{i-1}}\right)|00\rangle + \sin(\theta_{\vec{b}_{i-1}})|11\rangle\right], \quad (9)$$

where the angles $\theta_{\vec{b}_{i-1}}$ and the matrix $U_A^{\vec{b}_{i-1}}$ both depend on the outcomes $\vec{b}_{i-1}$, on the initial angle θ_1 and the angles ξ_j of the previous B_j's with $j<i$. In the notation, we will always omit the dependence on the angles θ_1 and $\xi_1,\xi_2,\ldots,\xi_j$ since these are fixed *before* the beginning of the experiment. For each of these different potential states with angle $\theta_{\vec{b}_{i-1}}$, Alice adds two measurements to her input choices, where for $k\in\{0,1\}$, these are measurements of the observables $\mathbb{A}_k^{\vec{b}_{i-1}}$ which are defined as

$$U_A^{\vec{b}_{i-1}}\left[\cos\left(\mu_{\vec{b}_{i-1}}\right)\sigma_z + (-1)^k \sin\left(\mu_{\vec{b}_{i-1}}\right)\sigma_x\right]\left(U_A^{\vec{b}_{i-1}}\right)^\dagger, \quad (10)$$

where $\tan(\mu_{\vec{b}_{i-1}})=\sin(2\theta_{\vec{b}_{i-1}})$, depending on the specific state $|\psi^{(i)}_{\vec{b}_{i-1}}\rangle$ in Eq. (9).

We are now ready to describe how the scheme certifies randomness. The measurement operator $\hat{\sigma}_x(\xi_i)$ can be made arbitrarily close to σ_x by choosing ξ_i sufficiently small. This brings the outcome statistics for measurements $\hat{\sigma}_x(\xi_i),\sigma_z$ on Bob's side and $\mathbb{A}_0^{\vec{b}_{i-1}},\mathbb{A}_1^{\vec{b}_{i-1}}$ on Alice's side on the state in Eq. (9), arbitrarily close to the statistics for the measurements in Eq. (5) and a state of the form in Eq. (3), for $\theta=\theta_{\vec{b}_{i-1}}$. Therefore, the inequality $I_{\theta_{\vec{b}_{i-1}}}$ for Alice and B_i as defined in Eq. (4) can be made arbitrarily close to its maximal violation. This in turn guarantees that the guessing probability $G(y_i^0=1,P_{\text{obs}})$ can be made arbitrarily close to $1/2$. Note that this guessing probability does not only describe the instances when Alice chooses the measurements $\mathbb{A}_j^{\vec{b}_{i-1}}$. Since Eve does not know Alice's measurement choices in advance she cannot use a strategy that gives higher predictive power for the instances when Alice chooses other measurements. Finally, by making $G(y_i^0=1,P_{\text{obs}})$ sufficiently close to $1/2$ for each i (by choosing each ξ_i sufficiently close to 0) the DIGP $G(y_1^0,y_2^0,\ldots,y_n^0,P_{\text{obs}})$ can be made arbitrarily close to 2^{-n} (see Sec. 5 in the Supplemental Material for a proof).

At the end, Bob can produce m random bits by a suitably chosen sequence $\hat{\sigma}_x(\xi_i)$, $i\in\{1,2,\ldots,n\}$, of $n>m$ measurements. The certification only requires that each B_i occasionally chooses the projective measurement σ_z so that the whole statistics can be obtained. Note that Bob can choose σ_z with probability γ_i and $\hat{\sigma}_x(\xi_i)$ with probability $1-\gamma_i$ for γ_i as close to zero as he wants. Finally, note that the value of *each* inequality $I_{\theta_{\vec{b}_{i-1}}}$ between each B_i and A can be made as close as wanted to the maximal value $I^{\max}_{\theta_{\vec{b}_{i-1}}}$. Therefore, we can certify randomness for each measurement B_i in the sequence at the expense of increasing the number of measurements that Alice chooses from.

This protocol can also be used to certify any finite amount of randomness with some small but strictly nonzero noise robustness. Indeed, assume the goal is to certify m random bits. One can then run the protocol for $m'>m$ bits. By continuity, when adding a small but finite amount of noise the protocol will certify m random bits.

Conclusion. We have presented a scheme for certifying an unbounded amount of random bits from a single pair of entangled qubits in the scenario where one of the qubits is subjected to a sequence of measurements. Our work is in many respects a proof-of-principle result: First, it requires an exponentially increasing number of measurements on Alice's side, namely, $\sum_{i=1}^n 2^i = 2(2^n-1)$ measurement choices for n measurements in the sequence. Second, the result is based on a continuity argument and there is no control on the noise robustness. All these issues deserve further investigation. Finally, it is worth exploring how to design device-independent randomness generation protocols involving sequences of measurements. However, the sequential scenario is much more demanding from an implementation point of view, because it requires quantum nondemolition measurements. It is then unclear whether with present or near future technology, sequential protocols will provide a significant practical advantage over simpler protocols based on standard Bell tests. However, the first experimental works observing nonlocal correlations in the sequential scenario have recently been reported [19,20]. In any case, the main implications of our work are fundamental: It shows that a single pair of pure entangled qubits is a potentially unbounded source of certifiable random bits when performing sequences of measurements on it.

Acknowledgments. This work is supported by the ERC CoG QITBOX and AdG OSYRIS, the AXA Chair in Quantum Information Science, Spanish MINECO (FOQUS FIS2013-46768-P and SEV-2015-0522), Fundación Cellex, Generalitat de Catalunya (SGR 875), and The John Templeton Foundation. M.J. acknowledges support from the Marie Curie COFUND action through the ICFOnest program. R.A. acknowledges funding from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie Grant Agreement No. 705109. M.J.H. acknowledges support from the EPSRC (through the NQIT Quantum Hub) and the FQXi Large Grant Thermodynamic vs Information Theoretic Entropies in Probabilistic Theories. P.W. acknowledges computational resources granted by the High Performance Computing Center North (SNIC 2015/1-162 and SNIC 2016/1-320).

[1] J. S. Bell, Physics **1**, 195 (1964).
[2] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[3] L. Masanes, A. Acín, and N. Gisin, Phys. Rev. A **73**, 012112 (2006).
[4] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
[5] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature **464**, 1021 (2010).
[6] R. Colbeck, Ph.D. thesis, University of Cambridge, 2006.
[7] U. Vazirani and T. Vidick, Philos. Trans. R. Soc. London A **370**, 3432 (2012).
[8] R. Colbeck and R. Renner, Nat. Phys. **8**, 450 (2012).
[9] R. Gallego, L. Masanes, G. De La Torre, C. Dhara, L. Aolita, and A. Acín, Nat. Commun. **4**, 2654 (2013).
[10] G. M. D'Ariano, P. L. Presti, and P. Perinotti, J. Phys. A **38**, 5979 (2005).
[11] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, Phys. Rev. A **93**, 040102 (2016).
[12] R. Gallego, L. E. Würflinger, R. Chaves, A. Acín, and M. Navascués, New J. Phys. **16**, 033037 (2014).
[13] S. Popescu, Phys. Rev. Lett. **74**, 2619 (1995).
[14] A. Acín, S. Massar, and S. Pironio, Phys. Rev. Lett. **108**, 100402 (2012).
[15] O. Nieto-Silleras, S. Pironio, and J. Silman, New J. Phys. **16**, 013035 (2014).
[16] G. de la Torre, M. J. Hoban, C. Dhara, G. Prettico, and A. Acín, Phys. Rev. Lett. **114**, 160502 (2015).
[17] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevA.95.020102 for the proofs of continuity of any guessing probability function $G(y^0, P_{\text{obs}})$ close to a unique point of maximal violation, and the proof that the guessing probability of n sequential binary measurement outcomes can be arbitrarily close to 2^{-n}. It also contains a numerical upper bound on $G(y^0, P_{\text{obs}})$ by a concave function of the value of I_θ.
[18] R. Silva, N. Gisin, Y. Guryanova, and S. Popescu, Phys. Rev. Lett. **114**, 250401 (2015).
[19] M. Schiavon, L. Calderaro, M. Pittaluga, G. Vallone, and P. Villoresi, arXiv:1611.02430.
[20] M.-J. Hu, Z.-Y. Zhou, X.-M. Hu, C.-F. Li, G.-C. Guo, and Y.-S. Zhang, arXiv:1609.01863.